УДК 004.457
DOI 10.21685/2587-7704-2019-4-1-13

Open Access | RESEARCH ARTICLE

# Применение средств защиты информации от несанкционированного доступа для защиты ПЭВМ, функционирующих под управлением операционной системы Linux

***Р. К. Коновалов***
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

***А. Г. Фатеев***
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

**Аннотация**. Проведен анализ возможности применения средств защиты информации от несанкционированного доступа (НСД) для защиты ПЭВМ, функционирующих под управлением операционной системы Linux. Сделан обзор и проведен анализ средств защиты информации (СЗИ) от НСД, имеющих сертификат ФСТЭК. Проведенный анализ показал, что существующие СЗИ позволяют реализовать защиту информации от НСД для защиты ПЭВМ, функционирующих под управлением операционной системы Linux в полном объеме. Однако количество СЗИ, имеющих сертификат ФСТЭК, на данный момент крайне мало.

**Ключевые слова**: операционная система, средства защиты информации, информационная безопасность, несанкционированный доступ, Linux.

# The use of information security products against unauthorized access to protect PC running under the Linux operating system

***R. K. Konovalov***
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

***A. G. Fateev***
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

**Abstract**. An analysis of possibility to use information security products against unauthorized access (UA) to protect PC running under the Linux operating system has been carried out. A review and analysis of information security products (ISP) against UA certified by the FSTEC was made. The analysis showed that the existing ISP allows implementing the information protection against UA to secure PC operating under the Linux operating system in full. However, the amount of ISP having the FSTEC certificate is currently extremely small.

**Keywords**: operating system, information security products, information security, unauthorized access, Linux.

В основном средства защиты информации (СЗИ) разрабатывались для защиты персональных компьютеров на базе операционной системы (ОС) MicrosoftWindows. Поскольку дистрибутивы ОС Linux не имели широкого распространения ранее, то и в СЗИ для данной ОС не было острой необходимости, они почти не разрабатывались. В связи с тем, что в федеральных и муниципальных органах вла-

сти предполагается отказаться от использования коммерческой ОС MicrosoftWindows и начать использование бесплатной ОС Linux, то возникла потребность в разработке СЗИ от несанкционированного доступа (НСД) для ОС Linux. Компании-разработчики начали работу в этом направлении. Такие СЗИ представлены на рынке на сегодняшний день, но в малом количестве. Операционная система Linux все больше применяется, и все больше возникает потребность в подготовке администраторов, имеющих навыки по развертыванию, настройке и эксплуатации средств защиты информации на базе ОС Linux.

Обзор и анализ СЗИ от НСД для ОС Linux проводился с использованием государственного реестра сертифицированных СЗИ [1]. Было установлено, что набор СЗИ от НСД, работающих под управлением ОС Linux, ограничивается двумя продуктами: «СЗИ от НСД Dallas Lock Linux» и «СЗИ от НСД Secret Net LSP», а также двумя электронными замками, которые имеют возможность работать на ПЭВМ с любой установленной ОС. Электронные замки рассматриваться не будут, потому что они имеют ограниченный функционал.

СЗИ от НСД Dallas Lock Linux – сертифицированная система защиты конфиденциальной информации накладного типа – предназначена для автономных персональных компьютеров и компьютеров в составе локально-вычислительной сети.

Представляет собой программный комплекс СЗИ от НСД для ОС семейства Linux с возможностью подключения аппаратных идентификаторов, легко интегрируется в сложные сетевые инфраструктуры, благодаря собственному набору сертифицированных решений.

Изделие предназначено для комплексной и многофункциональной защиты информационных ресурсов от НСД при работе в многопользовательских автоматизированных системах (АС), информационных системах персональных данных (ИСПДн), автоматизированных системах управления производственными и технологическими процессами (АСУ ТП), государственных информационных системах (ГИС).

Изделие соответствует требованиям руководящих документов (Требования безопасности информации ФСТЭК России):

– «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» по 5-му классу защищенности;

– «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по 4-му уровню контроля.

Изделие может быть использовано:

– при создании защищенных автоматизированных систем до класса защищенности 1Г включительно (Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации»);

– в государственных информационных системах 1-го класса защищённости (Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждени Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»);

– для обеспечения 1-го уровня защищенности персональных данных (Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»);

– при создании защищенных информационных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды до 1-го класса защищенности включительно (Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды») [2].

СЗИ от НСД SecretNetLSP является сертифицированным средством защиты информации от НСД и позволяет привести АС на платформе Linux в соответствие требованиям регулирующих документов:

– Приказ ФСТЭК России от 11.02.2013 № 17 – требования по защите информации в ГИС;

– Приказ ФСТЭК России от 18.02.2013 № 21 – требования по защите персональных данных в ИСПДн;

– Приказ ФСТЭК России от 14.03.2014 № 31 – требования по защите информации в АСУ ТП на критически важных объектах [3].

В общем и целом СЗИ сопоставимы, так как оба СЗИ от НСД построены для выполнения одних и тех же требований по ЗИ, но Secret Net LSP дает большую свободу для специалиста ИБ в планировании информационной инфраструктуры организации и построении ее защиты.

Продукт компании «Код Безопасности» Secret Net LSP поддерживает большее количество ОС, в том числе сертифицированные российские разработки Astra Linux.

Кроме обзора СЗИ от НСД, были рассмотрены положения ФСТЭК [4–6], и анализ показал, что СЗИ от НСД SecretNet LSP обеспечивает реализацию большинства мер защиты, кроме таких, как:

– ограничение программной среды (ОПС);
– антивирусная защита (АВЗ);
– обнаружение вторжений (СОВ);
– обеспечение доступности (ОДТ);
– защита технических средств (ЗТС);
– выявление инцидентов и реагирование на них (ИНЦ);
– управление конфигурацией информационной системы и системы защиты (УКФ).

Также существует ряд мер защиты из других наборов, которые не могут быть реализованы СЗИ от НСД Secret Net LSP, например идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных (ИАФ.2), идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) (ИАФ.6), контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны (ЗНИ.3) и др. Оценка показывает, что СЗИ от НСД Secret Net LSP позволяет реализовать почти половину мер защиты, установленных положениями ФСТЭК [4–6].

В сравнении СЗИ от НСД для ОС Linux и СЗИ от НСД для ОС MicrosoftWindows было выявлено, что набор функций почти совпадает, но СЗИ от НСД Secret Net LSP немного уступает набором функций версиям для операционной системы Microsoft Windows. Несмотря на то, что некоторые меры защиты не реализуются, средства защиты информации могут применяться для защиты информации при работе на ПЭВМ под управлением операционных систем на базе Linux.

## Библиографический список

1. Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 // fstec.ru : официальный сайт ФСТЭК Росии. – URL: https://fstec.ru/tekhnicheskaya-zaschita-informatsii/dokumenty-po-sertifickatsii/153-sistema-sertifikatsii/591(свободный).
2. СЗИ НСД Dallas Lock Linux // www.dallaslock.ru : официальный сайт разработчиков. – URL: https://www.dallaslock.ru/products/szi-nsd-dallas-lock-linux/ (свободный).
3. СЗИ от НСД Secret Net LSP // www.securitycode.ru: официальный сайт разработчиков. Режим доступа: https://www.securitycode.ru/products/szi_secret_net/ (свободный).
4. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : Приказ ФСТЭК России от 18 февраля 2013 г. № 21 // fstec.ru : официальный сайт ФСТЭК Росии. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691(свободный).
5. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : Приказ ФСТЭК России от 11 февраля 2013 г. № 17 // fstec.ru : официальный сайт ФСТЭК Росии. – URL : https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702 (свободный).
6. Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды : Приказ ФСТЭК России от 14 марта 2014 г. № 31 // fstec.ru : официальный сайт ФСТЭК России. – URL: https://fstec.ru/index?id=868:prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (свободный).

**Образец цитирования:**

Коновалов, Р. К. Применение средств защиты информации от несанкционированного доступа для защиты ПЭВМ, функционирующих под управлением операционной системы Linux / Р. К. Коновалов, А. Г. Фатеев // Инжиниринг и технологии. – 2019. – Vol. 4(1). – С. 1–3. – DOI 10.21685/2587-7704-2019-4-1-13.